Carnegie Mellon University
CyLab

Governance of Enterprise Security:
CyLab 2012 Report

How Boards & Senior Executives
Are Managing Cyber Risks

Author: Jody R. Westby
Adjunct Distinguished Fellow, CyLab
CEO, Global Cyber Risk LLC

May 16, 2012

Research Sponsors:

RSA

Forbes

Carnegie Mellon CyLab

Carnegie Mellon University

5000 Forbes Avenue

Pittsburgh, PA 15213

(412) 268-5090 • (412) 268-7675 (Fax)

Dean, College of Engineering & Founder, CyLab: Pradeep K. Khosla, Ph.D.

Director, CyLab: Virgil Gligor

Adjunct Distinguished Fellow: Jody R. Westby

Jody R. Westby, Esq.

CEO

Global Cyber Risk LLC

5125 MacArthur Blvd., NW

Third Floor

Washington, DC 20016

(202) 537-5070 • (202) 537-5073 (Fax)

Table of Contents

Abbreviations

ABA	American Bar Association
ASIS	American Society for Industrial Security
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMU	Carnegie Mellon University
CoE	Council of Europe
COO	Chief Operating Officer
CPO	Chief Privacy Officer
CRO	Chief Risk Officer
CSO	Chief Security Officer
CyLab	Carnegie Mellon CyLab
D&Os	Directors & Officers
eGRC	Enterprise Governance, Risk, and Compliance
EU	European Union
FDA	Food and Drug Administration
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
HITECH Act	Health Information Technology for Economic and Clinical Health Act
HIPAA	Health Insurance Portability and Accountability Act
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISSA	Information Systems Security Association
IT	Information Technology
ITU	International Telecommunication Union
ITGI	Information Technology Governance Institute
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NSF	National Science Foundation
PII	Personally Identifiable Information
PwC	PricewaterhouseCoopers
R&D	Research & Development
SEC	Securities and Exchange Commission
SIEM	Security Information and Event Management
SOD	Segregation of Duties
U.S.	United States

About Carnegie Mellon CyLab

Carnegie Mellon CyLab is one of the largest university-based cybersecurity research and education centers in the U.S. CyLab is located in the College of Engineering at Carnegie Mellon University and has campuses in Silicon Valley and Pittsburgh.

Carnegie Mellon CyLab is a bold and visionary effort, which establishes public-private partnerships to develop new technologies for measurable, secure, available, trustworthy, and sustainable computing and communications systems. CyLab is a world leader in both technological research and the education of professionals in information assurance, security technology, business and policy, as well as security awareness among cybercitizens of all ages.

Building on more than two decades of Carnegie Mellon leadership in Information Technology, CyLab is a university-wide initiative that involves more than 50 faculty and 100 graduate students from more than six different departments and schools.

CyLab is:

- A National Science Foundation (NSF) CyberTrust Center
- Affiliated with CERT, at the Software Engineering Institute
- A key partner in NSF-funded Center for Team Research in Ubiquitous Secure Technology
- A National Security Agency (NSA) Center of Academic Excellence in Information Assurance Education and a Center for Academic Excellence in Research.

About Jody R. Westby

Drawing upon a unique combination of more than 20 years of technical, legal, policy, and business experience, Ms. Westby provides consulting and legal services to public and private sector clients in the areas of privacy, security, cybercrime, breach management, and IT governance. Her services include governance assistance to boards and senior management, security risk assessments, global compliance reviews, security investigations, and high-value data protection evaluations. Her company, Global Cyber Risk LLC, is a preferred provider of privacy and security consulting services to Reed Smith.

Ms. Westby serves as Adjunct Distinguished Fellow at Carnegie Mellon CyLab. She was lead author on Carnegie Mellon's *Governing for Enterprise Security Implementation Guide,*[1] which was developed for boards and senior management, and its 2008 and 2010 *Governance of Enterprise Security Survey* reports. Ms. Westby's work for Carnegie Mellon on the governance responsibilities of boards and senior executives for the security of their organizations' systems and data has been showcased by the CISO Executive Network and Bloomberg BNA's *Privacy & Security Law Report.*

Prior to founding Global Cyber Risk, Ms. Westby served as senior managing director for PricewaterhouseCoopers (PwC) where she was responsible for information security, privacy, information sharing, and critical infrastructure protection issues across the federal government. She also was co-lead in launching their outsourcing practice. Before joining PwC, Ms. Westby founded the Work-IT Group, and specialized in serving government and private sector clients on legal and regulatory issues associated with information technology and online business. Ms. Westby has advised government officials and industry in countries around the world on the development of their legal frameworks for e-commerce and security.

Previously, Ms. Westby launched In-Q-Tel, an IT solutions/venture capital company founded by the CIA, was Senior Fellow & Director of IT Studies for the Progress & Freedom Foundation, and was Director of Domestic Policy for the U.S. Chamber of Commerce. She also practiced law with the New York firms of Shearman & Sterling and Paul, Weiss, Rifkind, Wharton & Garrison.

Ms. Westby is a professional blogger for Forbes on cybersecurity and privacy issues. She is chair of the American Bar Association's (ABA) Privacy and Computer Crime Committee and was chair, co-author and editor of its *International Guide to Combating Cybercrime, International Guide to Cyber Security, International Guide to Privacy,* and *Roadmap to an Enterprise Security Program* (endorsed by the Global CSO Council). She was editor and co-author of the 2010 UN publication, *The Quest for Cyber Peace* and is author of two books on legal issues associated with cybersecurity research.

She is co-chair of the World Federation of Scientists' Permanent Monitoring Panel on Information Security and was appointed to the United Nations' ITU High Level Experts Group on Cybersecurity. She also serves on the advisory board of *The Intellectual Property Counselor* and Bloomberg BNA's *Privacy and Security Law Report.* Ms. Westby is a member of the bars of the District of Columbia, Colorado, and Pennsylvania, and of the ABA. She received her B.A., *summa cum laude*, from the University of Tulsa and her J.D., *magna cum laude*, from Georgetown University Law Center. She is a member of the Order of the Coif, the American Bar Foundation, and the Cosmos Club.

About RSA

Founded in 1982, **RSA, The Security Division of EMC**, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention, Continuous Network Monitoring, and Fraud Protection with industry-leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform, and the data that is generated.

RSA's industry leading-solutions are designed to work together to create a systematic approach to managing security, risk and compliance – eliminating the hundreds of security and compliance silos that exist in most organizations today. Our technology solutions for physical, virtual and cloud computing environments include:

- *Authentication* – A wide range of strong two-factor authentication solutions to help organizations assure user identities and meet compliance requirements.
- *Access Control* – Access control solutions manage access, federate identities and enforce organizational policies across multiple web resources, portals and applications.
- *Data Loss Prevention*—Identify and enforce policies to prevent the loss or misuse of sensitive data – whether at rest in a data center, in motion over the network, or in use on a laptop or desktop.
- *Encryption, Tokenization, and Key Management*— Secures sensitive data stored in file systems on servers and endpoints and at the point of capture. RSA key management solutions simplify the provisioning, distribution, and management of encryption keys.
- *Fraud Prevention*—Reduces the risk of fraud and identity theft by assuring user identities, monitoring for high-risk activities, and mitigating the damage caused by external threats such as phishing, pharming, Trojans, and other cyber threats.
- *Enterprise Governance, Risk and Compliance*—Helps to manage the lifecycle of corporate policies and objectives by analyzing and responding to enterprise risk and demonstrating compliance with a real-time view into the state of compliance and risk level.
- *Network security monitoring*—Provides real-time visibility into network traffic and log event activity for a precise and actionable understanding of everything happening on the network. Enables organizations to identify, prioritize, and remediate complex IT risks, gain efficiencies in their incident management process and improve their overall operational effectiveness.
- *Security Information and Event Management*—Transforms raw log and event data into critical information to help organizations simplify compliance, identify and respond to high-risk events, and optimize IT and network operations.

For more information, please visit www.RSA.com and www.EMC.com.

About Forbes

Forbes Media encompasses Forbes and Forbes.com<http://Forbes.com> (www.forbes.com<http://www.forbes.com>), the leading business site on the Web that reaches on average 30 million people monthly. The company publishes Forbes, Forbes Asia and Forbes Europe, which together reach a worldwide audience of more than six million readers. It also publishes ForbesLife magazine, in addition to licensee editions in Africa, Argentina, Bulgaria, China, Croatia, Czech Republic, Estonia, Georgia, India, Indonesia, Israel, Kazakhstan, Korea, Latvia, Middle East, Poland, Romania, Russia, Slovakia, Turkey, and Ukraine.

Other Forbes Media Web sites are:

ForbesWoman.com	http://ForbesWoman.com
RealClearPolitics.com	http://RealClearPolitics.com
RealClearMarkets.com	http://RealClearMarkets.com
RealClearSports.com	http://RealClearSports.com
RealClearWorld.com	http://RealClearWorld.com.

Together with Forbes.com, http://Forbes.com, these sites reach on average 36 million business decision makers each month.

Steve Forbes serves as Chairman and Editor in Chief. Mike Perlis is President and Chief Executive Officer. Lewis D'Vorkin is Chief Product Officer. Meredith Kopit Levien is Chief Revenue Officer.

Executive Summary

It has long been recognized that directors and officers have a fiduciary duty to protect the assets of their organizations. Today, this duty extends to digital assets, and has been expanded by laws and regulations that impose specific privacy and cybersecurity obligations on companies.

This is the third biennial survey that Carnegie Mellon CyLab has conducted on how boards of directors and senior management are governing the security of their organizations' information, applications, and networks (digital assets). First conducted in 2008 and carried forward in 2010 and 2012, the surveys are intended to measure the extent to which cyber governance is improving. The 2012 survey is the first global governance survey, comparing responses from industry sectors and geographical regions.

57% of respondents are not analyzing the adequacy of cyber insurance coverage or undertaking key activities related to cyber risk management to help them manage reputational and financial risks associated with the theft of confidential and proprietary data and security breaches.

The CyLab 2012 survey is based upon results received from 108 respondents at the board or senior executive level from Forbes Global 2000 companies. Half of the respondents are board members, and the other half are non-director senior executives. Twenty-four percent (24%) of the respondents are board chairs and 44% are on board Audit, Governance, or Risk Committees. Seventy-five percent (75%) of the respondents are from critical infrastructure companies.

For the third time, the survey revealed that boards are not actively addressing cyber risk management. While placing high importance on risk management generally, there is still a gap in understanding the linkage between information technology (IT) risks and enterprise risk management. Although there have been some measureable improvements since the 2008 and 2010 surveys, boards still are not undertaking key oversight activities related to cyber risks, such as reviewing budgets, security program assessments, and top-level policies; assigning roles and responsibilities for privacy and security; and receiving regular reports on breaches and IT risks. Involvement in these areas would help them manage reputational and financial risks associated with the theft of confidential and proprietary data and security breaches of personal information.

Improvements are largely organizational. There has been a noticeable increase in the number of boards with Risk Committees responsible for privacy and security risks (48% in 2012 compared with 8% in 2008) and in the number of companies that have established cross-organizational teams to manage privacy and security risks (72% in 2012 compared with 17% in 2008). Boards and senior management are lagging, however, in

establishing key positions for privacy and security and appropriately assigning responsibilities. *Less than two-thirds of the Forbes Global 2000 companies responding to the survey have full-time personnel in key roles for privacy and security (CISO/CSO, CPO, CRO) in a manner that is consistent with internationally accepted best practices and standards.* An amazing 82% of the respondents indicated that they did not have a CPO. In addition, the majority of CISOs (58%) and 47% of CSOs are assigned responsibility for both privacy and security and tend to report to the CIO, creating segregation of duties (SOD) issues that are against best practices.

Despite these organizational improvements, respondents indicated that Audit Committees and full boards are still mostly responsible for oversight of risk. The report highlights the SOD issues that arise when Audit Committees both oversee the development of security programs and also audit the controls and effectiveness of such programs.

Although most boards (89%) review risk assessments, less than half of them hire outside expertise to assist with risk management. Only 16% of board Risk Committees and 16% of IT Committees hire outside experts. Despite 91% of the respondents indicating that risk management was being actively addressed by the board, the issues that received the least attention were IT operations (29%), computer and information security (33%), and vendor management (13%). The continuing low scores in these areas indicate that boards do not understand that, today, all business operations are supported by computer systems and digital data, and that risks in these areas can undermine operations. The low response for vendor management is concerning because it indicates that the privacy and security of data at cloud and software providers and outsource vendors are receiving little oversight.

Another positive sign from the survey was the importance that boards are placing upon IT and security/risk expertise in board recruitment. Results indicated that IT expertise was very important or important for 37% of the respondents and somewhat important for 42%. Risk and security expertise was even more encouraging, with 64% of the respondents indicating that it was very important or important and 27% indicating it was somewhat important.

"Another positive sign from the survey was the importance that boards are placing upon IT and security/risk expertise in board

INDUSTRY SECTOR COMPARISONS

Industry sector and regional comparisons from the survey provide interesting insights into how privacy and security risks are managed among critical infrastructure industry sectors and across geographical regions. *The survey confirmed the belief among security experts that, overall, the financial sector has better privacy and security practices than other industry sectors.* Respondents indicated that the financial sector paid more attention to IT and security issues and was more engaged in best practice activities, such as budget reviews, roles and responsibilities, and top-level policies, than the energy/utilities, IT/telecom, and industrials industry sectors. The financial sector also has a higher rate of (1) board IT/Technology Committees, and (2) Risk Committees separate from the Audit Committee that have responsibility for privacy and security.

The IT/telecom sector tends not to establish board IT/Technology Committees and assigns privacy and security oversight responsibilities to their Audit Committees. The energy/utilities and industrials sector respondents each indicated that their boards never (0%) address vendor management issues, whereas the financial and IT/telecom respondents said they do (28% and 15%, respectively). Energy/utilities respondents also ranked the lowest in establishing board Risk Committees separate from the Audit

Committee, but indicated that when they do form a Risk Committee, they assign it responsibility for privacy and security. Only half of the energy/utilities and infrastructure sectors indicated that they have cross-organizational committees.

Respondents indicated that all industry sectors surveyed are not properly assigning privacy responsibilities to CPOs. None of the IT/telecom respondents (0%) indicated that they had a CPO, even though they have some of the most stringent privacy and security compliance requirements, and only seven percent (7%) of the energy/utilities respondents said they had a CPO. Just 13% of industrials sector respondents said they had a CPO, and 17% of the financial sector respondents said they did.

Interestingly, none of the energy/utilities sector respondents (0%) indicated that they have a CRO even though their risks are high. The energy/utilities sector also places a much lower value on board member IT experience than the other sectors, which is puzzling since their operations are so dependent upon complex supervisory control and data acquisition (SCADA) systems.

The energy/utilities and IT/telecom sector boards also are not reviewing cyber insurance coverage (79% and 77%, respectively) compared to the financial sector (52% not reviewing) and industrials sector (44% not reviewing) boards. The industrials sector respondents indicated that they exclusively (100%) rely upon insurance brokers to provide outside risk expertise, while the energy/utilities and IT/telecom sectors never do (0% for each). The financial sector respondents indicated that they seldom use insurance brokers for this purpose.

Regional Comparisons

Although Europe leads globally in privacy regulation and enforcement, few European organizations have a CPO (3%), with Asia only slightly ahead at five percent (5%) and North America at 23%. European companies, however, are more likely to have CISOs and CSOs (72%) than North American or Asian organizations (58% and 52%, respectively).

North American boards lag behind European and Asian boards in undertaking key activities associated with privacy and security governance. European boards, however, pay less attention to IT operations and computer and information security (19%) than North American and Asian boards (40% and 38%, respectively).

Boards across geographical regions were even in their neglect to review cyber insurance coverage (56-58%).

Asian boards (76%) are much more likely to have a board Risk Committee responsible for privacy and security than North American and European boards (35% and 41%, respectively). Asian organizations (82%) are much more likely to have privacy responsibilities assigned to security personnel than North American and European organizations (44% and 48%, respectively). Asian organizations are less likely to have the CISO/CSO report to the CIO, however.

RECOMMENDATIONS

The survey revealed that governance of enterprise security is still lacking in most corporations, with gaps in critical areas. If boards and senior management take the following 12 actions, they could significantly improve their organizations' security posture and reduce risk:

1. Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks. Recruit directors with security and IT governance and cyber risk expertise.
2. Ensure that privacy and security roles within the organization are separated and that responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management.
3. Evaluate the existing organizational structure and establish a cross-organizational team that is required to meet at least monthly to coordinate and communicate on privacy and security issues. This team should include senior management from human resources, public relations, legal, and procurement, as well as the CFO, the CIO, CISO/CSO, CRO, the CPO, and business line executives.
4. Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cybersecurity and the protection of privacy and viewing it as a corporate social responsibility.
5. Review assessments of the organization's security program and ensure that the program comports with best practices and standards and includes incident response, breach notification, disaster recovery, and crisis communications plans.
6. Ensure that privacy and security requirements for vendors (including cloud and software-as-a-service providers) are based upon key aspects of the organization's security program, including annual audits and control requirements. Carefully review notification procedures in the event of a breach or security incident.
7. Conduct an annual audit of the organization's enterprise security program, to be reviewed by the Audit Committee.
8. Conduct an annual review of the enterprise security program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed.
9. Require regular reports from senior management on privacy and security risks.
10. Require annual board review of budgets for privacy and security risk management.
11. Conduct annual privacy compliance audits and test incident response, breach notification, disaster recovery, and crisis communication plans.
12. Assess cyber risks and potential loss valuations and review adequacy of cyber insurance coverage.

About the Survey

Carnegie Mellon University's Dean of Engineering and Founder of CyLab, Pradeep Khosla, sent personal letters to board members and senior executives from the Forbes Global 2000 list of companies, asking them to complete a brief survey designed to help Carnegie Mellon understand how boards and business leaders are managing risk, particularly technology-related risks. Only one response per company was used in calculating response rates.

The CyLab 2012 report on *Governance of Enterprise Security* is based upon 108 responses, representing a response rate of 5.4% out of a total of 1,989 surveys (based on one per company). One half of the respondents were board members: forty-eight percent (48%) were inside directors and two percent (2%) were outside directors. Twenty-four percent (24%) of these directors were board chairs. The remaining half of the respondents were senior executives, but not a board member.

Since respondents may serve on several boards, the survey asked them to select only one organization as the focus of their responses and to base all of their answers on that one organization.

The findings were analyzed according to actual responses, i.e., percentages reflect the number of participants who responded to the particular question, rather than the total number of participants.

Please note that this survey is exploratory in nature and is based on voluntary (rather than randomly selected) respondents, and that these findings do not purport to represent the entire population of directors.

CyLab and Jody Westby wish to gratefully acknowledge the contribution of Steve Fienberg, Chair of the Statistics Department and Maurice Falk University Professor of Statistics and Social Science, Carnegie Mellon University, and Benjamin McGrath, a CMU student, who assisted in the development of the survey, the calculation of the survey results, and finalization of this report.

I. Introduction

Purpose of the Governance Survey

CyLab's first biennial *Governance of Enterprise Security Survey* (Governance Survey) was conducted in 2008, and the second in 2010. The surveys have been consistent and designed to determine:

- Whether the claims of IT professionals that their boards and senior management were not paying attention to the security of their organizations' data and information technology (IT) systems were valid
- The degree to which boards of directors and officers (D&Os) were actually managing privacy and cybersecurity risks
- The board and organizational structure for such governance
- The degree to which companies were following best practices for privacy and security.

The results of the 2008 and 2010 Governance Surveys confirmed that:

- Boards and executives were not exercising adequate oversight of the privacy and security of their systems and data
- Most companies did not have privacy and security executives
- Most organizations were not engaging in key privacy and security activities that would help protect the organization from risk.

The CyLab 2010 and 2012 Governance Surveys asked similar questions to determine whether governance over digital assets has improved. The 2012 report measures the progress made and identifies areas where boards and senior executives need to improve their oversight, and compares, where possible, the results from 2008 and 2010.

Background: Duty of Boards & Directors

The governance responsibilities of D&Os have been in the spotlight since 2002 with the fall of Enron and Arthur Andersen and the enactment of Sarbanes-Oxley. The economic collapse in 2008-09 drew even more attention to board and executive responsibility for the management of risk. In addition, (1) natural disasters that have disrupted operations, (2) headlines that have resulted from data breaches, and (3) the loss of confidential and proprietary information from sophisticated cyber attacks have caused D&Os to wonder if their operations and data are secure and if corporate response plans are adequate.

The dependency of all organizations upon information systems and global networks has extended governance responsibilities to the use of IT. What is IT governance? The IT Governance Institute (ITGI) states that:

> *IT governance* is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.[2]

Enterprise governance and IT governance increasingly encompass the security of IT systems and information. The American Society for Industrial Security (ASIS), the Information Systems Security Association (ISSA), and the Information Systems Audit and Control Association (ISACA) note in their report, *Convergence of Enterprise Security Organizations,* that:

> As new technologies emerge and threats become increasingly complex and unpredictable, senior security executives recognize the need to merge security functions throughout the entire enterprise.[3]

It has long been recognized that D&Os have a fiduciary duty to protect the assets of their organizations.[4] Today, this duty extends to "digital assets" – information, applications, and networks. This duty has been expanded by the enactment of state and federal laws and regulations that impose specific privacy and security requirements on targeted industry sectors and types of data. For example, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and state breach laws impose specific requirements pertaining to the security and privacy of data and networks.

"Corporate data is at a higher risk of theft or misuse than ever before, and the systemic nature of recent attacks has alarmed both industry leaders and government officials around the world."

Sarbanes-Oxley requires both management and external auditors to attest to the effectiveness of internal controls that provide meaningful assurance about the security of information assets.[5] In late 2011, the Securities and Exchange Commission (SEC) issued guidelines that require public companies to disclose the risk of cyber incidents if they materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, or if they make an investment in the company speculative or risky.[6]

The pressure on critical infrastructure industry sectors to secure their systems according to best practices and standards persists, with the U.S. energy sector already subject to regulations.[7] Today, the tone in Washington has moved from persuasive to compulsory, with numerous bills pending in Congress that mandate security measures for corporate systems if enacted.[8]

In addition, the reputational and financial consequences of a breach can be significant. When a company is the victim of an attack on its information systems – whether from an insider or an outside bad actor – studies have shown that this can result in a lack of confidence in the company and even a drop in the company stock price.[9] Breaches of personally identifiable information (PII) are expensive and frequently result in civil and class action lawsuits and investigation by state attorneys general or the Federal Trade Commission. The 2011 *U.S. Cost of a Data Breach Study*, conducted by Symantec and the Ponemon Institute, calculated that data breaches cost companies an average of USD5.5 million per incident.[10] Another recent Ponemon survey found that brand and reputation can decline 17-31% after a breach, and that it may take an organization more than a year to recover its corporate image.[11]

Corporate data is at a higher risk of theft or misuse than ever before, and the systemic nature of recent attacks has alarmed both industry leaders and government officials around the world. *Managing these cyber risks now*

requires active oversight by boards and senior executives. Failure to properly govern cybersecurity and privacy may result in shareholder derivative suits against D&Os for breach of fiduciary duty as a result of losses on stock price, decrease in market share, or damage to brand caused by inadequate attention to the security of the company's data, applications, and networks. Although Delaware case law provides strong protections to D&Os under the business judgment rule and recent case law,[12] harm caused by security breaches *may* receive stricter scrutiny because:

- Security best practices and standards are well-developed, harmonized, and widely available;
- Many privacy and security laws require organizations to have an enterprise security program that is regularly reviewed and tested;
- The Council of Europe Convention on Cybercrime,[13] which has been signed by 47 countries and ratified by 33 (including the U.S.), holds companies civilly, administratively, or criminally liable for cybercrimes that benefit the company and were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director. Article 9 of the European Union's (EU) Council Framework Decision on attacks against information systems,[14] which applies to all 27 EU member countries, mirrors the CoE language.

Thus, D&O duties with respect to privacy and security may be more prescribed in this area and negligence more easily proven. There are also situations where higher standards apply to directors and officers, such as acquisitions, takeovers, responses to shareholder suits, and distribution of assets to shareholders in preference over creditors. In these circumstances, directors and officers are required to obtain professional assistance or perform adequate analyses to mitigate the risks that ordinarily accompany these activities. Some information assurance experts assert that a "higher degree of care will also be required of Directors and Officers regarding the complex nature of issues involved in information assurance."[15]

In addition, securities laws and regulations also require public corporations to adequately disclose the risks relevant to the corporation and its assets in their public filings. The *Independent Director* put this in the context of information systems by reporting that:

> Management of information risk is central to the success of any organization operating today. For Directors, this means that Board performance is increasingly being judged by how well their company measures up to internationally accepted codes and guidelines on preferred Information Assurance practice.[16]

Clearly, directors and officers need to undertake a certain level of involvement and oversight in ensuring that the organization is properly secured and data is protected.

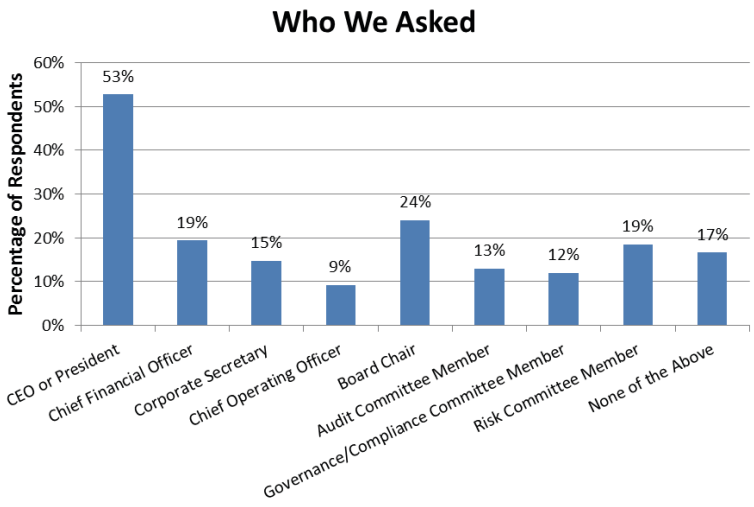
Fortunately, boards and senior executives have access to standards and best practices that guide them in fulfilling their governance responsibilities. The IT Governance Institute has an excellent collection of materials, as does ISACA, and Carnegie Mellon University. In addition, the International Organization for Standardization (ISO) has released ISO 38500, the international standard for corporate governance of IT, and the National Institute of Standards and Technology (NIST) has produced world-class materials on privacy and security best practices and guidance – including risk management – that are available at no cost.

II. Findings and Conclusions

WHO WE ASKED

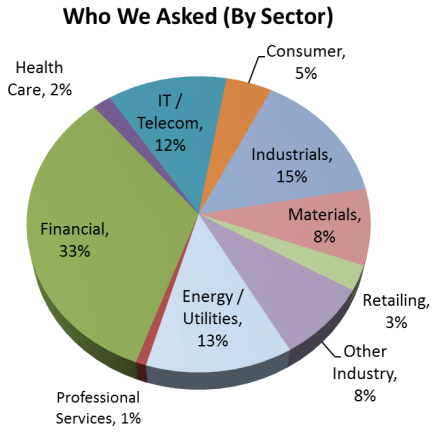
The Governance Survey respondents were half board members, half senior executives.
Forty-eight percent (48%) of respondents were inside directors and two percent (2%) were outside directors. Twenty-four percent (24%) of these directors were board chairs. The remaining half of the respondents were senior executives, but not a board member.
The respondents also indicated that:

- 13% of respondents were Audit Committee members;
- 12% of respondents were a Governance, Compliance, or Ethics Committee member; and
- 19% of respondents were Risk Committee members.



Internal respondents were holding positions as:
CEO or President (53%)
CFO (19%)
COO (9%)
Corporate Secretary (15%).

The majority of Governance Survey respondents (75%) were from critical infrastructure industry sectors which increasingly face government pressure and/or regulatory compliance requirements with respect to the security of their IT systems and data. These survey respondents represented:



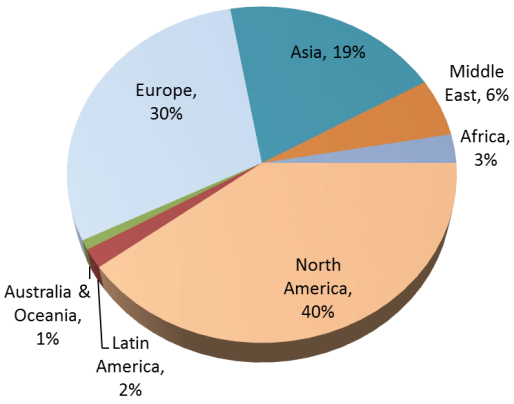
- Energy and utility companies – 13%
- Financial sector – 33%
- Health care – 2%
- Industrials – 15%
- IT and telecommunications companies – 12%.

The remaining 25% of respondents represented consumer, materials, professional services, retailing, and other types of companies.

Responses from four industrial sectors are compared in this report: energy/utilities, financial, IT/telecom, and industrials.

Survey respondents represented large to very large corporations. Since the respondent pool was drawn from the Forbes Global 2000 list, the respondents represented large or very large corporations. Almost half (49%) of respondents were from very large corporations with annual revenues greater than USD10 billion. Thirty-seven percent (37%) of the Governance Survey respondents came from large companies with annual revenues ranging between USD2.5 billion and USD10 billion, and 9% of respondents represented companies with revenues between USD1 billion and USD2.5 billion. Six percent (6%) of the respondents had revenues of USD500 million to less than USD1 billion.

Who We Asked (By Region)



Using the Forbes Global 2000 list, the 2012 survey represents the first analysis of cyber governance postures of major corporations around the world. Regions were aligned with those used by Internet World Stats to enable analysis of responses against Internet usage.[17] Responses were primarily from three geographical regions: North America (40%), Europe (30%), and Asia (19%), although a few responses were also received from Latin America, Australia and Oceania, the Middle East, and Africa. Responses from three regions are compared in this report, with key countries noted below by Internet usage:

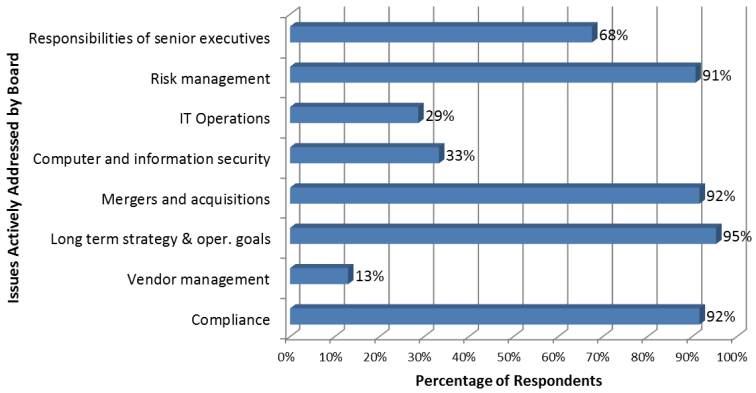
North America: United States and Canada.
Europe: EU countries, Russia, Turkey, Ukraine, and Switzerland.
Asia: China, India, Japan, Indonesia, South Korea, Philippines, Vietnam, Pakistan, and Thailand.

FINDINGS

Oversight & Governance

For the third time, the survey revealed that boards are actively addressing risk management, but that there is still a gap in understanding the linkage between IT risks and enterprise risk management.

Boards Still Not Actively Addressing IT, Security, Vendor Management



Although 91% of respondents indicated that risk management was being actively addressed by their board, the areas receiving the least attention were IT operations (29%), computer and information security (33%), and vendor management (13%). The lack of attention to vendor management is particularly concerning since this includes outsourcing of IT operations and business processes, most of which is dependent upon IT systems. These three issue areas held the same position in the 2010 results.

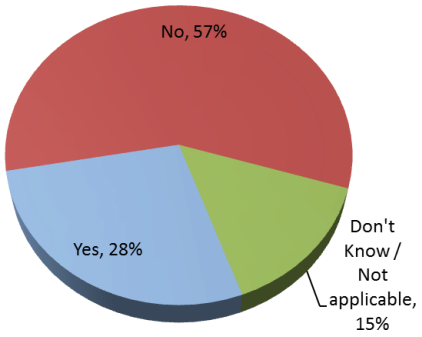
Industry & Region Comparison Table: Issues Actively Addressed By Boards

Issue Addressed By Boards	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
Vendor Mgmt	12%	9%	10%		0%	28%	15%	0%
Computer & Info Sec	40%	19%	38%		29%	44%	31%	13%
IT Operations	30%	19%	24%		14%	36%	31%	19%

European respondents gave the least attention to computer and information security (19%), compared to North American and Asian respondents at 40% and 38% respectively. Europe also was lowest in the attention given to IT operations (19%), compared to 30% for North America and 24% for Asia.

The financial sector showed the greatest degree of attention to these critical issues related to cyber risk management. One of the most revealing gaps is the lack of attention given to these issues by the energy/utilities and industrials sectors, particularly considering the degree to which operations and processes are controlled by IT systems.

Boards Not Reviewing Insurance Coverage for Cyber Risks



Even though risk management is a high priority, most boards are not reviewing their company's insurance coverage for cyber-related risks.

Although cyber incidents are not covered by general liability policies, 57% of the respondents indicated that their boards are not reviewing insurance coverage for cyber related risks, compared with 65% in 2010. This slight improvement, however, is due to the increase in respondents in 2012 that said they did not know. The response was consistent across geographical regions.

Industry & Region Comparison Table: Boards NOT Reviewing Cyber Insurance Coverage

Board reviews cyber insurance coverage?	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
No	58%	56%	57%		79%	52%	77%	44%

It was surprising that a much higher percentage of respondents from the two "consequential" infrastructure sectors[18] – energy/utilities and IT/telecom – indicated that their boards did not review insurance coverage of cyber risks: Seventy-nine percent (79%) of the energy/utilities respondents indicated that their boards do not review coverage and 77% of the IT/telecom sector respondents said the same.

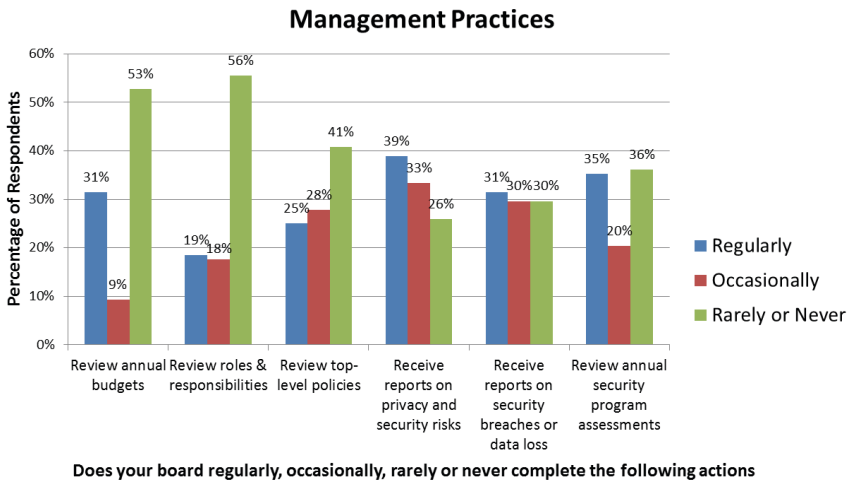
For the third time, the Governance Survey confirmed the belief among IT security professionals that boards and senior executives still are not involved in key areas related to governance over privacy and security. Although 89% of respondents said their boards review annual risk assessment reports and 91% of these cover computer systems and data, this activity alone is not adequate oversight.

Respondents indicated that boards are not focusing on important activities that would help protect the organization from some of its highest risks: the reputational and financial losses flowing from theft of confidential or proprietary data or security breaches involving the disclosure of PII. There are a number of

best practices for board involvement with respect to IT governance that strengthen the security posture of a company.

When asked whether their boards receive information or are involved in activities related to these best practices, respondents indicated that boards are only occasionally, rarely or never engaged:

- Review annual budgets. Fifty-three percent (53%) of respondents said their board rarely or never reviewed and approved annual budgets for privacy and IT security programs; 9% said they occasionally did. Only 31% of respondents indicated that their boards regularly reviewed and approved these budgets.
- Review roles and responsibilities. Fifty-six percent (56%) of respondents indicated their board rarely or never reviewed and approved roles and responsibilities of personnel responsible for privacy and security risks; an additional 18% said they occasionally did. Only 19% said they regularly reviewed privacy and security roles and responsibilities.



- Review top-level policies. Forty-one percent (41%) of respondents said their board rarely or never reviewed and approved top-level policies regarding privacy and security risks; an additional 28% said they occasionally did. Only one-quarter (25%) of the respondents said they regularly reviewed top-level privacy and security policies.
- Receive reports on privacy and security risks. Twenty-six percent (26%) of respondents said their board rarely or never received reports from senior management regarding privacy and IT security risks; an additional 33% said they occasionally got such reports. Thirty-nine percent (39%) said they regularly received reports on privacy and IT security risks. These results were slightly better than the 2008 results (62% occasionally or rarely received reports and 15% never did).
- Receive reports on security breaches or loss of data. Thirty percent (30%) of respondents said their board rarely or never reviewed reports of security breaches or incidents involving the disclosure of personally identifiable information or theft of corporate data; another 30% said they occasionally received such reports. Thirty-one percent (31%) of the respondents said their boards regularly reviewed these reports.
- Review annual computer security program assessments. Thirty-six (36%) of respondents said their board rarely or never reviewed annual security program assessments; another 20% said they occasionally did. Only 35% of the respondents said they regularly reviewed such reports.

There were only modest gains in each of the first four areas (breach reports and security program assessments were not asked for in the 2008 and 2010 surveys), particularly in regularly receiving reports from senior

management regarding privacy and security risks (20% in 2008 compared with 39% in 2012) and reviewing budgets (14% in 2008 compared with 31% in 2012).

Industry & Region Comparison Table: Boards Rarely or Never Undertaking Best Practice Activities

Percentage of boards that rarely or never:	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
Rarely/never review annual budgets	81%	44%	29%		71%	42%	62%	56%
Rarely/never review roles & responsibilities	67%	53%	43%		79%	39%	69%	75%
Rarely/never review top-level policies	56%	38%	33%		64%	19%	54%	63%
Rarely/never receive privacy/security reports	23%	31%	24%		21%	11%	31%	50%
Rarely/never receive breach/data loss rpts	14%	44%	52%		36%	22%	31%	44%
Rarely/never review security program assessments	37%	34%	48%		57%	17%	46%	50%

North American respondents indicated that their boards are more neglectful in undertaking key activities associated with privacy and security governance than European and Asian boards, except for receiving reports. European respondents are worse at undertaking best practices than Asian respondents, except for reviewing breach reports and security program assessments.

In examining sector responses, the financial sector far outpaced other industry sectors in every area, confirming the view that they lead in good governance practices, although budget reviews should improve. The survey respondents indicated that the energy/utilities industry sector has the poorest governance in every area except for receiving reports.

Board Committee Structure

Some of the biggest improvements have been organizational. Traditionally, boards have not separated risk management and audit responsibilities by establishing separate Risk and Audit Committees. Although the majority of companies still tend to place risk responsibilities with the Audit Committee, the Governance Surveys show this is changing. How a board is organized and how it assigns committee responsibilities can significantly influence the effectiveness of its management activities and security posture.

Respondents indicated that only 48% of boards have a Risk Committee that is separate from an Audit Committee – and of these, 81% of these Risk Committees oversee privacy and security. These results represent a significant improvement since the 2008 survey, when only 8% of boards had Risk Committees and only 53% of those oversaw privacy and security, and the 2010 survey, which indicated 14% of boards had a Risk Committee and of those, 67% of them had oversight of privacy and security.

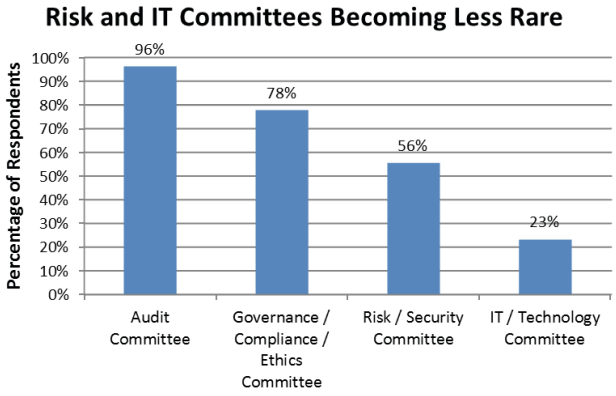
Industry & Region Comparison Table: Risk Committees Responsible for Privacy & Security

Risk Committee Separate from Audit?	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
Yes	35%	41%	76%		35%	78%	31%	44%
If yes, does the Risk Committee oversee privacy & security?								
Yes	93%	85%	75%		100%	79%	75%	57%

The survey indicates that Asia is far ahead of North America and Europe in understanding the importance of having a Risk Committee separate from the board Audit Committee, but more North American companies assign privacy and security risks to these Risk Committees than Asian companies.

The financial sector respondents indicated that they are much farther ahead in establishing Risk Committees (78%), but only about three-fourths of them (79%) are responsible for privacy and security. Even though the energy sector was next to last in establishing Risk Committees (35%), 100% of them are assigned privacy and security oversight.

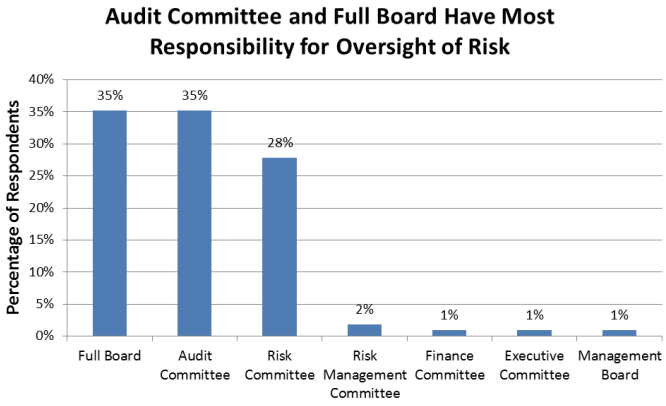
Board committee structures are starting to form around security and technology risks.
Not surprisingly, 96% of the survey population said their boards have an Audit Committee and 78% of them have a Governance, Compliance, or Ethics Committee. When polled about the types of committees their boards have, respondents indicated that 56% of boards have a Risk/Security Committee and 23% have an IT/Technology Committee. This shows improvement from the 2010 survey results, which indicated that only 12% of respondents had a Risk/Security Committee and 6% had an IT/Technology Committee.



Industry & Region Comparison Table: Board Committee Structures

Boards have these committees?	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
Have Risk/Security Committee	28%	59%	95%		36%	86%	46%	63%
Have IT/Technology Committee	16%	21%	38%		14%	39%	0%	13%

Asian respondents indicated that their boards are way ahead of North America and Europe in understanding the need for both Risk/Security Committees (95%) and IT/Technology Committees (38%), while North America surprisingly lags behind at 28% and 16% respectively. The energy/utilities sector respondents indicated that they have the fewest Risk/Security Committees, but IT/telecom respondents revealed that their sector does not have any (0%) IT/Technology Committees. This is surprising on both counts, since energy/utility companies are critical infrastructure subject to security regulations and the IT/telecom industry relies upon technology and IT systems for its revenue. Not surprisingly, the financial sector again led the way in understanding the need for these board committees.



When asked who was most responsible for the oversight of risk, about one-third of the respondents (35%) indicated the Audit Committee, while an equal number of respondents (35%) indicated that the full board was responsible. The 2008 survey revealed that the Audit Committee was

responsible for risk 65% of the time and the full board 22%, while the 2010 survey indicated the Audit Committee had responsibility for risk 53% of the time and the full board had responsibility 22% of the time.

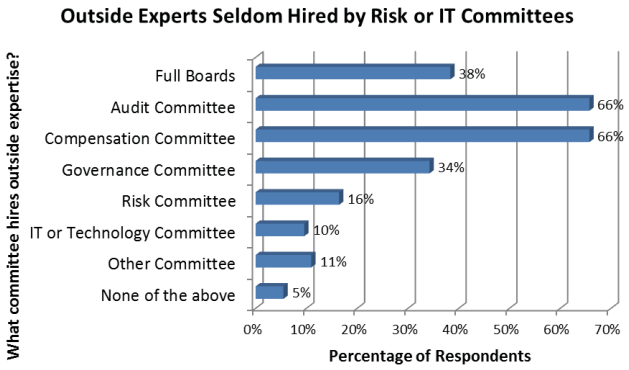
The 2012 results indicate a clear shift away from assigning the Audit Committee the most responsibility for risk. The 2012 survey indicates the Risk Committee has responsibility for risk 30% of the respondents, whereas in 2010 it was only 5% and in 2008 it was 4%. Best practices and industry standards separate the audit and risk functions. The 2008 and 2010 surveys indicated an over-reliance upon Audit Committees to manage risk issues, creating segregation of duties (SOD) issues at the board level since the same committee that exercised oversight of operational aspects of privacy and security also oversaw audits in these areas. Carnegie Mellon's *Governing for Enterprise Security Implementation Guide* provides step-by-step guidance on Risk Committee responsibilities for managing IT security risks.[19]

Industry & Region Comparison Table: Most Responsibility for Cyber Risks

Who has most responsibility for risk?	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
Full Board	33%	34%	48%		43%	31%	23%	44%
Audit Committee	42%	41%	14%		43%	11%	54%	25%
Risk Committee	23%	22%	38%		14%	58%	23%	25%

Interestingly, 54% of the IT/telecom sector respondents indicated that the Audit Committee has the most responsibility for risk, while the financial sector indicated just the opposite, with 58% of the respondents saying that the most responsibility for risk falls to the Risk Committee.

Board Risk and IT Committees rarely hire outside expertise.



Although 68% of the respondents indicated that their boards engage outside consultants, legal counsel, or other experts, they also said these experts are primarily hired by the Audit, Compensation, or Governance Committees or by the full board. *Risk and IT/Technology Committees only hire outside expertise 16% and 10% of the time, respectively.* The lower percentage, however, may be due to the small number of board Risk and IT Committees. This is some improvement, though. In 2010, only 5% of the respondents indicted their Risk Committee hired outside expertise.

Less than half of boards hire outside experts to help with risk assessments and risk management. Although 89% of the respondents indicated their boards reviewed risk assessment reports, only 46% of the respondents said that their boards hire outside expertise to assist with risk assessments and risk management. Less than one third (30%) of the respondents indicated this expertise came from risk services firms, 27% of the respondents said it came

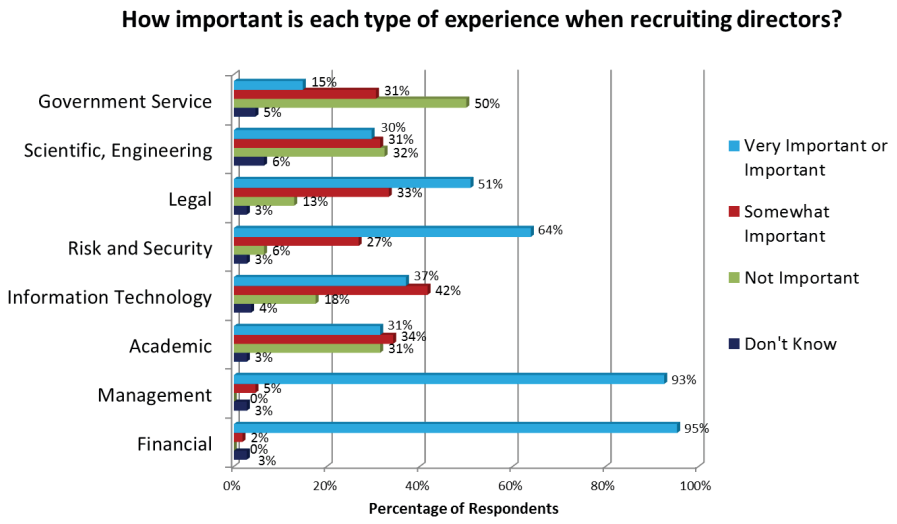
from IT security experts, and 18% said insurance brokers provided outside expertise. In the 2010 survey, 17% of the respondents indicated that IT security experts provided outside expertise, while 26% indicated insurance brokers provided these services, just the opposite of the 2012 survey. It is important to note that the survey did not ask what topics the outside experts were asked to address, so it is possible that the Audit, full board, or other committees hired computer security or IT expertise.

Industry & Region Comparison Table: Board Use of Outside Experts

Source of outside risk expertise	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
Risk Services Firm	36%	23%	30%		17%	40%	0%	20%
Insurance Broker	45%	8%	15%		0%	10%	0%	100%
IT Security Experts	36%	39%	15%		50%	20%	33%	20%

The North American respondents indicated that they are clearly more reliant upon insurance brokers to provide outside expertise than Europe or Asia. It is interesting to note, however, that respondents from the energy/utilities and IT/telecom sectors said they do not use insurance brokers at all for outside expertise, while 100% of the respondents from the industrials sector indicated that they use insurance brokers for this purpose.

IT security and risk experience becoming more valuable to boards.



Twenty-seven percent (27%) of the respondents indicated that their board had an outside director with cybersecurity expertise, up from 18% in 2010. Seventy-three percent (73%) of the respondents said their boards had an outside director with risk expertise, compared with 59% in 2010. Fifty-one percent (51%) of respondents indicated that their boards retain professional search firms to seek qualified candidates for their board.

Not surprisingly, the experience deemed most important in recruiting directors was financial and management expertise. IT expertise is becoming more valuable, however. When recruiting, IT expertise was very important or important for 37% of the respondents and somewhat important for 42%. *It is encouraging that 64% of the respondents indicated that risk and security expertise was either very important or important and 27% said it was somewhat important.*

Industry & Region Comparison Table: Experience Valuable When Recruiting Board Members

When recruiting board members, how valuable is:	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
IT experience – Very imp or imp	42%	22%	48%		7%	42%	62%	31%
Risk/security experience – Very imp or imp	63%	56%	62%		50%	75%	69%	50%

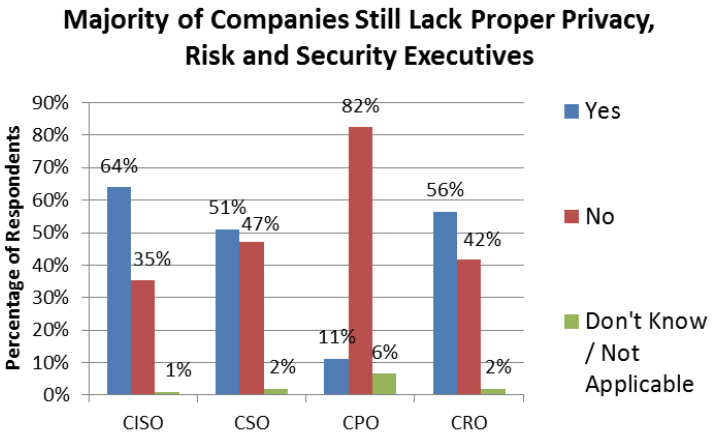
Only 22% of European respondents indicated that IT experience was very important or important in recruiting board members, while 42% of North American and 48% of Asian respondents indicated it was very important or important. Only 7% of the respondents from the energy/utilities sector found IT experience to be very important or important, while other sectors ranked it quite high, especially the IT/telecom sector.

Internal Organizational Roles & Responsibilities

Boards and senior management are lagging in establishing key positions for privacy and security or appropriately assigning responsibilities.

Best practices call for clear roles and responsibilities with respect to privacy and security. The delineation of responsibilities should serve as a check and balance and protect the company against SOD issues that could increase risk. There is a general belief that most companies do not understand this and are not creating the needed roles or are inappropriately combining responsibilities. So disparate are the approaches to IT security, that titles for personnel responsible for privacy and security span four possibilities: chief privacy officer (CPO), chief information security officer (CISO), chief security officer (CSO), and chief risk officer (CRO).

Organizations continued to show that they do not have full-time, senior-level personnel in place to appropriately manage privacy and security risks.



- 35% of the respondents said their organizations did not have a CISO
- 47% said they did not have a CSO
- 82% said they did not have a CPO
- 42% said their organizations did not have a CRO.

The CRO title is being used by security savvy companies that understand the need to integrate IT, physical, and personnel risks and manage them through one position. *Less than two-thirds of the Forbes Global 2000 companies responding to the survey have full-time personnel in key roles responsible for privacy and security in a manner that is consistent with internationally accepted best practices and standards.*

It is possible that some respondents indicated that they did not have someone in a particular position because the person in their organization did not have that specific title. This, however, does not comport with best practices and standards. *Any organization large enough to be included in the Forbes Global 2000 list should have a CIO, CISO/CSO, CPO, and CRO.* The percentage of companies without these positions was also high in the 2008 and 2010 surveys, although the number of organizations that do have CISOs jumped from 30% in 2008 and

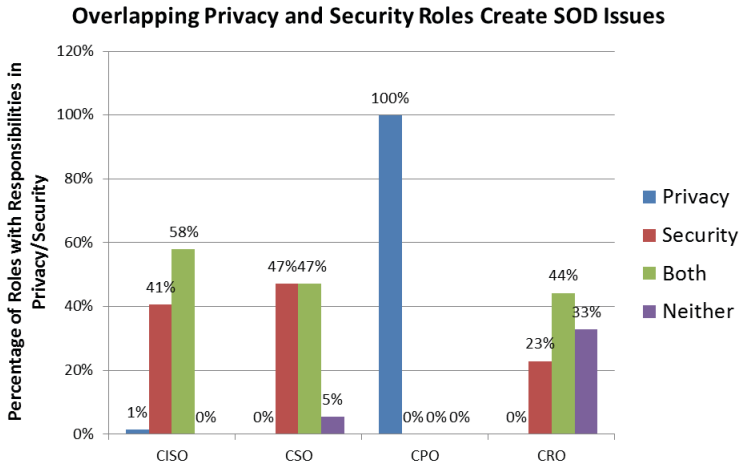
39% in 2010 to 64% in 2012. The number of organizations that have CSOs also gained from 16% in 2008 and 36% in 2010 to 51% in 2012. The CPO position is the most baffling. Only 7% of the respondents indicated they had a CPO in 2008, 18% said they did in 2010, and only 11% did in 2012. Clearly, this is an area that requires more board attention.

Industry & Region Comparison Table: Organizations with Privacy & Security Personnel

Percentage of companies that have:	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
CISO	58%	72%	52%		50%	81%	69%	50%
CSO	47%	63%	38%		50%	75%	69%	50%
CPO	23%	3%	5%		7%	17%	0%	13%
CRO	49%	56%	57%		57%	89%	54%	25%

With the European Union's strong emphasis on privacy, it is interesting to note that 23% of the North American respondents indicated that their organization has a CPO, while only 3% of the European respondents indicated that they do, but Europe had a higher percentage of CISOs and CSOs than North America. The low rate of CISOs/CSOs for the energy/utilities sector is also puzzling, since they are a highly regulated critical infrastructure sector, with energy grids subject to mandatory security regulations. It is also surprising that the IT/telecom respondents indicated that none of them have CPOs since they are subject to numerous privacy laws and regulations.

Organizations tend to overlap privacy and security responsibilities, not understanding the inherent SOD issues.



It is important that privacy and security responsibilities be separated to prevent a single point of failure, which can occur (a) when security personnel do not understand compliance requirements or needed privacy controls, or (b) when privacy personnel do not understand the technical security configuration or technical controls.[20] The 2012 survey respondents indicated that 58% of CISOs and 47% of CSOs are responsible for both privacy and security. Forty-four percent (44%) of CROs have both areas of responsibility. Interestingly, none (0%) of the respondents assigned security responsibilities to their CPO.

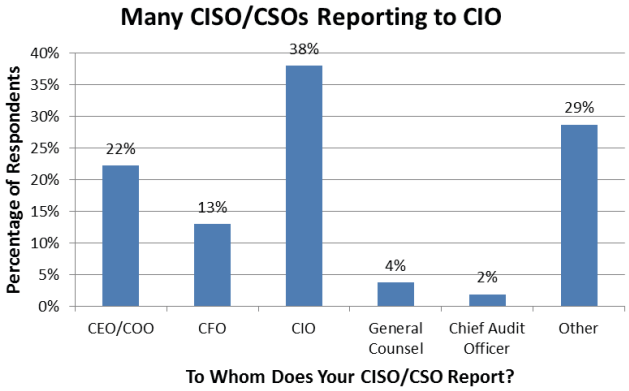
There are few differences between the 2008 and 2010 survey results on overlapping responsibilities that are noteworthy. The percentage of CISOs and CSOs responsible for both privacy and security has remained very high.

Industry & Region Comparison Table: Security Personnel Also Responsible for Privacy

Person also assigned privacy responsibilities	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
CISO	44%	48%	82%		43%	76%	78%	25%
CSO	35%	40%	63%		38%	63%	67%	33%
CRO	48%	22%	67%		0%	56%	86%	0%

Asian respondents indicated that their CISOs, CSOs, and CROs, are much more likely to be responsible for both privacy and security than those in North America and Europe. The financial and IT/telecom industry sectors also are especially likely to double up on privacy and security responsibilities. Interestingly, neither the energy/utilities or industrials industry sectors ever assign privacy responsibilities to their CROs.

There are also SOD issues at line responsibility levels when CISOs/CSOs report to chief information officers (CIOs) because the CIO then controls the budget for the security program and may override security configuration decisions or policies in favor of his/her own infrastructure architecture preferences, thereby compromising security. In addition, the CIO may interfere with security procurements by favoring certain vendors or products without understanding the technological differences between the products. *Although such reporting relationships are against best practices, 38% of the respondents indicated that the CISO/CSO reported to the CIO in their organization.* Twenty-two percent (22%) of the respondents indicated that the CISO/CSO reported to the CEO and 13% indicated that the CISO/CSO reported to the CFO.



Industry & Region Comparison Table: CISO/CSO Reporting Lines

CISO/CSO reporting to	North America	Europe	Asia		Energy / Utilities	Financial	IT / Telecom	Industrials
CIO	44%	50%	19%		50%	42%	15%	25%
CEO	5%	13%	57%		7%	28%	54%	19%
CFO	23%	3%	5%		14%	3%	8%	44%

While almost half of North American (44%) and European (50%) respondents indicated that their organizations' CISO/CSOs reported to the CIO, Asia showed a clear preference not to establish such reporting lines, with 57% of the CISO/CSOs reporting to the CEO. The North American respondents indicated that the CFO is a favored second choice for CISO/CSO reporting, but Europe preferred the CEO. The IT/telecom industry also favored CEO reporting with 54% of their CISO/CSOs reporting to the CEO and only 8% to the CFO. The industrials sector showed a leadership role with 44% of CISO/CSOs reporting to the CFO and 19% reporting to the CEO.

Organizations are showing significant gains in cross-organizational communication.
One of the most significant improvements from the 2008 and 2010 Governance Surveys is in the establishment of internal cross-organizational groups for communicating about privacy and security issues. In 2008, only 17% of the respondents indicated that their organizations had a cross-organizational team; in 2010, 65% of the organizations did; and in 2012, 72% of the respondents indicated that such a committee had been established. This is very encouraging and indicates that companies are learning that cross-organizational communication is essential to addressing insider threats, combating external attacks, closing governance gaps, and reducing legal liability.

Industry & Region Comparison Table: Cross-Organizational Committees

Organizations with cross-Organizational committee	**North America**	**Europe**	**Asia**		**Energy / Utilities**	**Financial**	**IT / Telecom**	**Industrials**
	72%	72%	71%		50%	86%	92%	50%

The benefit of cross-organizational committees is realized across the globe; all geographic regions indicated that 71% or more organizations have a cross-organizational team. It is a different story within industry sectors, however. The energy/utilities and industrials sectors each indicated that only 50% of the organizations have such teams.

CONCLUSIONS

The following conclusions can be drawn from the findings of the 2012 CyLab Governance Survey:

- Boards are actively addressing risk management, but there is still a gap in understanding the linkage between cybersecurity risks and enterprise risk management.
- Boards are not undertaking key governance activities that would help protect their organizations from some of the highest risks: the reputational and financial losses flowing from theft of confidential and proprietary data or security breaches involving personally identifiable information.
- Organizationally, improvements are seen in (1) the increased number of boards with Risk Committees responsible for privacy and security risks, and (2) the high percentage of companies that have established cross-organizational committees to focus on privacy and security risks.
- Although most boards hire outside expertise, less than half hire it for assistance with risk assessments and risk management. There is a higher reliance upon IT security experts than risk services firms.
- The majority of boards are not evaluating the adequacy of their organizations' insurance coverage for cyber risks.
- Boards are recognizing that IT security and risk expertise are important skills when recruiting board members.
- Less than two-thirds of the Forbes Global 2000 companies responding to the survey have full-time personnel in key roles responsible for privacy and security in a manner that is consistent with internationally accepted best practices and standards. For organizations that do have these roles assigned, there is a serious lack of functional separation of privacy and security responsibilities.
- CISO/CSOs still tend to report to CIOs more than to CEOs or CFOs.

Regional Conclusions

- European boards pay less attention to IT operations and computer and information security than North American and Asian boards.
- Other than receiving privacy/security and breach/data loss reports, North American boards lag behind European and Asian boards in undertaking key activities associated with privacy and security governance.
- Asian boards are much more likely to have board Risk Committees responsible for privacy and security than North American and European boards.
- Across all regions, 56-58% of boards are not reviewing their organization's cyber insurance coverage.
- North American boards are much more reliant upon insurance broker risk expertise than risk services firms or IT security experts when seeking assistance with risk assessments and risk management.
- North American and Asian boards value board member IT experience much more highly than European boards. All geographical regions value risk and security expertise.
- Although Europe leads globally in privacy regulation and enforcement, few European organizations have a CPO (3%), with Asia only slightly ahead (5%). European companies, however, have a higher percentage of CISOs and CSOs than North American or Asian organizations.
- Asian organizations (82%) are much more likely to have privacy and security responsibilities assigned to key personnel than North American and European organizations (44% and 48%, respectively). Asians are less likely, however, to have the CISO/CSO report to the CIO.

Industry Sector Conclusions

- The financial sector has better privacy and security governance practices than the energy/utilities, IT/telecom, and industrials industry sectors. It also has a high rate of board IT/Technology Committees and Risk Committees separate from the Audit Committee, which are assigned oversight of privacy and security.
- Unlike the financial sector, the IT/telecom sector tends to assign the Audit Committee responsibility for cybersecurity and privacy risks.
- The IT/telecom industry sector respondents indicated that none of their organizations have a board IT/Technology Committee.
- The energy/utilities and IT/telecom respondents indicated that their organizations never (0%) rely upon insurance brokers to provide outside risk expertise, while the industrials sector relies upon them 100%. The financial sector seldom does.
- Energy/utilities and IT/telecom sector boards are not adequately reviewing cyber insurance coverage.
- The energy/utilities sector places a much lower value on board member IT experience than financial, IT/telecom, and industrials industry sectors.

- Zero percent (0%) of the IT/telecom industry sector said they have CPOs, even though they have some of the most stringent privacy compliance requirements. Likewise, none (0%) of the respondents from the energy/utilities and industrials sectors indicated they have CROs.

III. Recommendations

The survey revealed that governance of enterprise security is still lacking in most corporations, with gaps in critical areas. If boards and senior management take the following 12 actions, they could significantly improve their organizations' security posture and reduce risk:

1. Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks. Recruit directors with security and IT governance and cyber risk expertise.
2. Ensure that privacy and security roles within the organization are separated and that responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management.
3. Evaluate the existing organizational structure and establish a cross-organizational team that is required to meet at least monthly to coordinate and communicate on privacy and security issues. This team should include senior management from human resources, public relations, legal, and procurement, as well as the CFO, the CIO, CISO/CSO, CRO, the CPO, and business line executives.
4. Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cybersecurity and the protection of privacy and viewing it as a corporate social responsibility.
5. Review assessments of the organization's security program and ensure that the program comports with best practices and standards and includes incident response, breach notification, disaster recovery, and crisis communications plans.
6. Ensure that privacy and security requirements for vendors (including cloud and software-as-a-service providers) are based upon key aspects of the organization's security program, including annual audits and control requirements. Carefully review notification procedures in the event of a breach or security incident.
7. Conduct an annual audit of the organization's enterprise security program, to be reviewed by the Audit Committee.
8. Conduct an annual review of the enterprise security program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed.
9. Require regular reports from senior management on privacy and security risks.
10. Require annual board review of budgets for privacy and security risk management.
11. Conduct annual privacy compliance audits and test incident response, breach notification, disaster recovery, and crisis communication plans.
12. Assess cyber risks and potential loss valuations and review adequacy of cyber insurance coverage.

Endnotes

[1] Jody R. Westby & Julia Allen, *Governing for Enterprise Security Implementation Guide*, Carnegie Mellon University, Software Engineering Institute, Technical Note CMU/SEI-2000-TN-020, 2007, http://www.sei.cmu.edu/publications/documents/07.reports/07tn020.html (hereinafter "Westby & Allen").

[2] *Board Briefing on IT Governance,* 2nd ed., IT Governance Institute, 2003 at 10, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx (emphasis added).

[3] *Convergence of Enterprise Security Organizations,* American Society for industrial Security, Information Systems Security Association, and Information Systems Audit and Control Association, 2003 at 2, www.asisonline.org/newsroom/alliance.pdf.

[4] *See* Jody R. Westby, Testimony Before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Sept. 22, 2004, http://www.cccure.org/Documents/Governance/westby1.pdf . For a discussion regarding the fiduciary duty of boards and officers and the extension of that duty to protect the digital assets of their organizations, *see* Jody R. Westby, ed., *International Guide to Cyber Security,* American Bar Assn., Privacy & Computer Crime Committee, 2004 at 189-93.

[5] Sarbanes-Oxley Act of 2002, Pub. Law 107-204, Sections 302, 404, http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf. The SEC has taken a narrow interpretation of Sarbanes-Oxley to the point that information security and risk management pertain only to the financial statements of a company. The Federal Reserve has countered this by saying a broader interpretation is needed to include all of the operational risks since there are many aspects that can impact the financial standing of an organization that can affect the integrity and accuracy of the financials.

[6] "CF Disclosure Guidance: Topic 2, Cybersecurity," Securities and Exchange Commission, Division of Corporate Finance, Oct. 13, 2011, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[7] "Legal Resources," Critical Energy Infrastructure Information (CEII) Regulations, Federal Energy Regulatory Commission, http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp.

[8] *See, e.g.,* Jody Westby, "Cyber Legislation Will Cost Businesses and Hurt Economy," Feb. 27, 2012, *Forbes.com, http://www.forbes.com/sites/jodywestby/2012/02/27/cyber-legislation-will-cost-businesses-and-hurt-economy/*.

[9] Kevin Coleman, "Battle Damage Increases From Widespread Attacks," *Defense Systems,* Aug. 1, 2011, http://defensesystems.com/Articles/2011/07/18/Digital-Conflict-cyberattacks-economy-security.aspx?Page=1; Brian Cashell, William D. Jackson, Mark Jickling, Baird Webel, *The Economic Impact of Cyber-Attacks,"* Congressional Research Service, RL32331, Apr. 1, 2004, www.cisco.com/warp/public/779/.../images/CRS_Cyber_Attacks.pdf; A. Marshall Acuff, Jr., "Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business," Salomon Smith Barney, 2000, at 3-4.

[10] *2011 Cost of Data Breach Study: United States,* Ponemon Research Institute & Symantec Corp., Mar. 2012, http://www.symantec.com/about/news/release/article.jsp?prid=20120320_02.

[11] *Reputation Impact of a Data Breach: U.S. Study of Executives & Managers,* Ponemon Research Institute & Experian Corp., Nov. 2011, http://www.experian.com/blogs/data-breach/2012/01/17/how-data-breaches-harm-reputations/.

[12] In re *Citigroup Inc. Shareholder Derivative Action*, No. 3338-CC, 2009 WL 481906 (Del. Ch. Feb. 24, 2009), http://www.delawarelitigation.com/uploads/file/int99(1).pdf ; *Stone v. Ritter*, 911 A.2d 362, 366–67 (Del. 2006), http://caselaw.lp.findlaw.com/data2/delawarestatecases/93-2006.pdf.

[13] Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG, Council of Europe *Convention on Cybercrime Explanatory Report*, Nov. 8, 2001, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[14] *Proposal for a Council Framework Decision on attacks against information systems*, Commission of the European Communities, Article 9, Apr. 19, 2002, COM(2002) 173 final, 2002/0086 (CNS), http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf*; see also Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA,* European Commission, COM(2010) 517, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463.

[15] John H. Nugent, "Corporate Officer and Director Information Assurance (IA) Liability Issues: A Layman's Perspective," Dec. 15, 2002.

[16] *Id.* (citing Dr. Andrew Rathmell, Chairman of the Information Assurance Advisory Council, "Information Assurance: Protecting your Key Asset," http://www.iaac.ac.uk).

[17] *See* Internet World Stats, http://www.internetworldstats.com.

[18] Jody R. Westby, ed., *International Guide to Cyber Security,* ABA Publishing, American Bar Assn., 2004 at 18 (consequential infrastructure includes the information and communication systems that, when manipulated, could cause a catastrophic event with enormous consequences).

[19] Westby & Allen at 57-58.

[20] For a full discussion on the appropriate assignment of roles and responsibilities for all organizational personnel and boards of directors, *see* Westby and Allen at 19-31, Appendix C.